Projekt Interdyscyplinarny
Pozyskiwanie informacji ze źródeł zewnętrznych

dr inż. Marcin Luckner
mluckner@mini.pw.edu.pl

Wersja 1.1
12 października 2020

Biały wywiad

- Biały wywiad lub OSINT (ang. *Open Source Intelligence*).
  - forma **legalnego** wywiadu gospodarczego,
  - oparta o metodę pozyskiwania informacji z ogólnodostępnych źródeł.
    - środki masowego przekazu,
    - social media
  - wykorzystywany przez
    - agencje wywiadowcze,
    - policję,
    - prywatne wywiadownie gospodarcze.
- użyteczny również przy planowaniu testów penetracyjnych.

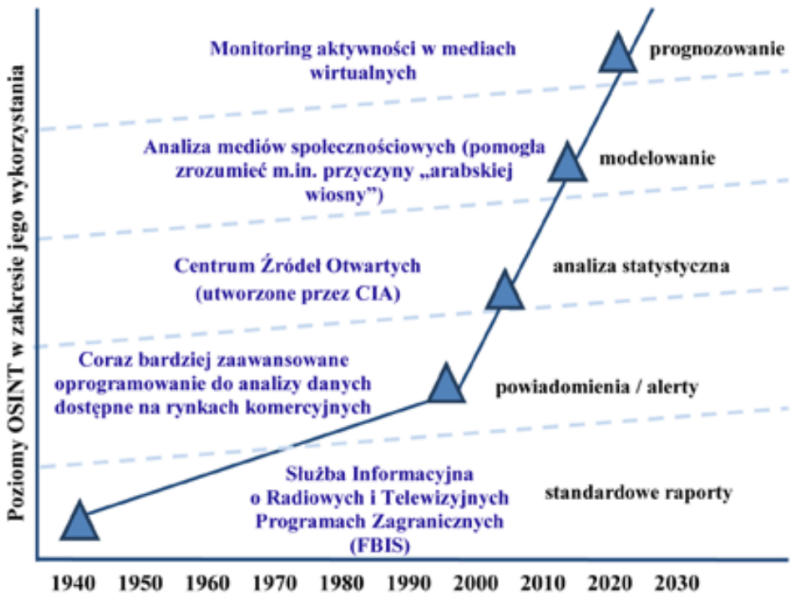
Historia - początki

- Georga Washington podczas rewolucji amerykańskiej czerpał aktualne informacje o sile brytyjskich wojsk i aktywności szpiegów z publikacji prasowych.
- Książę Wellington podczas Kampanii Iberyjskiej korzystał z codziennej prasy, w której szeroko opisywano sposób organizacji nowych struktur francuskiej piechoty.
- Podczas ofensywy we Francji wojska generała George'a Pattona w celu rozpoznania geoprzestrzennego używały map Michelin dostępnych na stacjach benzynowych.

Historia - profesjonalizacja

- W 1939 r. brytyjski rząd zwrócił się do BBC o utworzenie komercyjnego serwisu podsumowującego zagraniczną prasę i audycje radiowe.
- W 1941 r. decyzją prezydenta Franklina Delano Roosevelta utworzono w USA Służbę Monitoringu Nadawców Zagranicznych odpowiedzialną za monitorowanie, tłumaczenie, transkrypcję i analizę informacji pochodzących z audycji radiowych państw Osi.
- W czasie zimnej wojny Stasi analizowało miesięcznie około tysiąca zachodnich czasopism i 100 książek.
- W latach 50. XX w. Sherman Kent, twórca amerykańskiej szkoły analizy wywiadowczej, zamówił raport na temat stanu amerykańskiej armi sporządzony wyłącznie na podstawie źródeł otwartych. Raport w 90 proc. dawał właściwy obraz armii amerykańskiej, co spowodowało jego natychmiastowe utajnienie.

Rozwój OSINT



Rysunek 1: Rozwój OSINT [6]

- Współczesny biały wywiad rozszerzył swoją działalność na media społecznościowe.
- Celem jest już nie tylko analiza dostępnych danych, ale i ich wykorzystywanie do przewidywania przyszłych zdarzeń.

Dane osobowe

- Korzystanie z informacji ogólnodostępnych jest legalne, ale ich gromadzenie i przetwarzanie już niekoniecznie.
- Nieuprawnione wykorzystanie informacji sklasyfikowanych, jako dane osobowe podlega Ustawie o Ochronie Danych Osobowych i RODO (GDPR).
- W myśl tych przepisów, osoba prywatna powinna być poinformowana o fakcie i celu zbierania jej danych osobowych.
- Naruszenie przepisów może rodzić obowiązek wypłacenia odszkodowania i wiązać się z odpowiedzialnością karną.

Cele OSINT

- Celem białego wywiadu, jest pozyskanie na rzecz konkretnego podmiotu bądź na własne potrzeby oczekiwanych informacji z ewentualnym zamiarem dalszego ich przetwarzania.
- W działaniach biznesowych stosowany w celu oszacowania ryzyka współpracy z danym podmiotem.

OSINT w biznesie

- OSINT stosowany w biznesie skupia się na badaniu następujących aspektów przedsiębiorstwa:
  - sytuacja prawna,
    - Czy firma działa legalnie?
  - sytuacja finansowa,
    - Czy firma zachowuje płynność finansową?
  - sytuacja handlowa i ekonomiczna.
    - Kim są partnerzy firmy?

Interesujące informacje

- OSINT może obejmować:
  - szczegółowe dane firmowe dostępne w publicznych rejestrach,
  - sprawozdania finansowe publikowane w przypadku spółek akcyjnych,
  - kontakty pomiędzy dostawcami i klientami,
  - profile potencjalnych pracowników,
  - informacje o przetargach publicznych,
  - technologie wykorzystywane przez konkurencję.

Źródła danych

- Źródłem informacji mogą być:
  - krajowe i zagraniczne media (telewizja, radio, prasa),
  - serwisy informacyjne,
  - ogólnodostępne bazy danych,
  - platformy handlowe,
  - serwisy internetowe,
  - portale społecznościowe,
  - blogi i fora dyskusyjne,
  - mapy elektroniczne i papierowe,
  - biuletyny gospodarcze,
  - metadane, pozwalające na zidentyfikowanie obiektu cyfrowego (np. zdjęcia, filmu).

Wyszukiwarka Google

- Google
  - ogólne informacje o firmie.
- Google grafika
  - identyfikacja osób, miejsc.
- Google maps i street view.
  - weryfikacja deklarowanej siedziby firmy.

Wyszukiwarki z domeny cyber bezpieczeństwa

- WhoIs
  - rejestr domen internetowych
- WiGLE.net
  - baza aktywnych sieci wi-fi
- dnsbl.info
  - baza adresów rozsyłających spam
- shodan.io
  - skaner portów do pozyskiwania metadanych

Bazy przedsiębiorców

- Centralna Ewidencja i Informacja o Działalności Gospodarczej
  - `https://prod.ceidg.gov.pl/ceidg.cms.engine/`
- Krajowy Rejestr Sądowy
  - `https://ekrs.ms.gov.pl/web/wyszukiwarka-krs/strona-glowna/index.html`

Informacje o firmach

- Monitoring mediów
  - `www.brand24.pl`
- Notowania giełdowe
  - `www.stooq.pl`
- Dane o przetargach publicznych i konkursach na stanowiska publiczne
  - `www.bip.gov.pl`

Narzędzia OSINT

Tool	License	Input data	Platform
Maltego	MIT	Domain, username, url, email, image, DNS, IP, Location, phrase, etc.	Linux, Windows, Mac
Metagoofil	GNU 2.0	Url and type of file (extension), limit of results, etc.	Linux, Windows
The Foca	GPL 3.0	Type of file, domain, search engine, etc.	Linux, Windows
Shodan	MIT	Ip, country, port, keywords, hostname, DNS, protocol, url, etc.	Web
The Harvester	GPL 2.0	Domain, number of desired results, sources to search (Google, Bing, etc.)	Linux, Windows, Mac
Recon-NG	GNU 2.0	Domain, api-key, domain, special modules for gathering, etc.	Linux
Spiderfoot	GPL 2.0	Domain, username, files, url, email, etc.	Linux, Windows
Intel Techniques	N/A	Personal information (name, phone number, identification document, social network profile)	Web

Rysunek 2: Zestawienie narzędzi OSINT [4]

Omówienie narzędzi OSINT

- Maltego
  - Aplikacja do wyszukiwania, gromadzenia i graficznej prezentacji informacji publicznie dostępnych w sieci
- Wayback Machine Internet Archive
  - Cyfrowa baza zasobów dostępnych w internecie pozwalająca użytkownikom na przeglądanie zarchiwizowanych wersji witryn.
  - `web.archive.org`

Analiza rynku

- Analizą rynku pozwalają nam poznać i zrozumieć mechanizmy, zachowania i procesy rynkowe.
- Pozwala poznać bariery jakie trzeba pokonać, dopasować skalę działalności do potrzeb konsumentów, opracować właściwą strategię rozwoju.
- Analizie poddajemy najbliższe otoczenie przedsiębiorstwa jak i stan całego regionu.
  1. mikrootoczenie firmy
  2. makrootoczenie firmy

Analiza mikrootoczenia

- Analiza mikrootoczenia obejmuje poznanie:
  - konkurencji,
  - potencjalnych nabywców,
  - dostawców.
- Badanie mikro można przeprowadzić za pomocą 5 sił Portera.

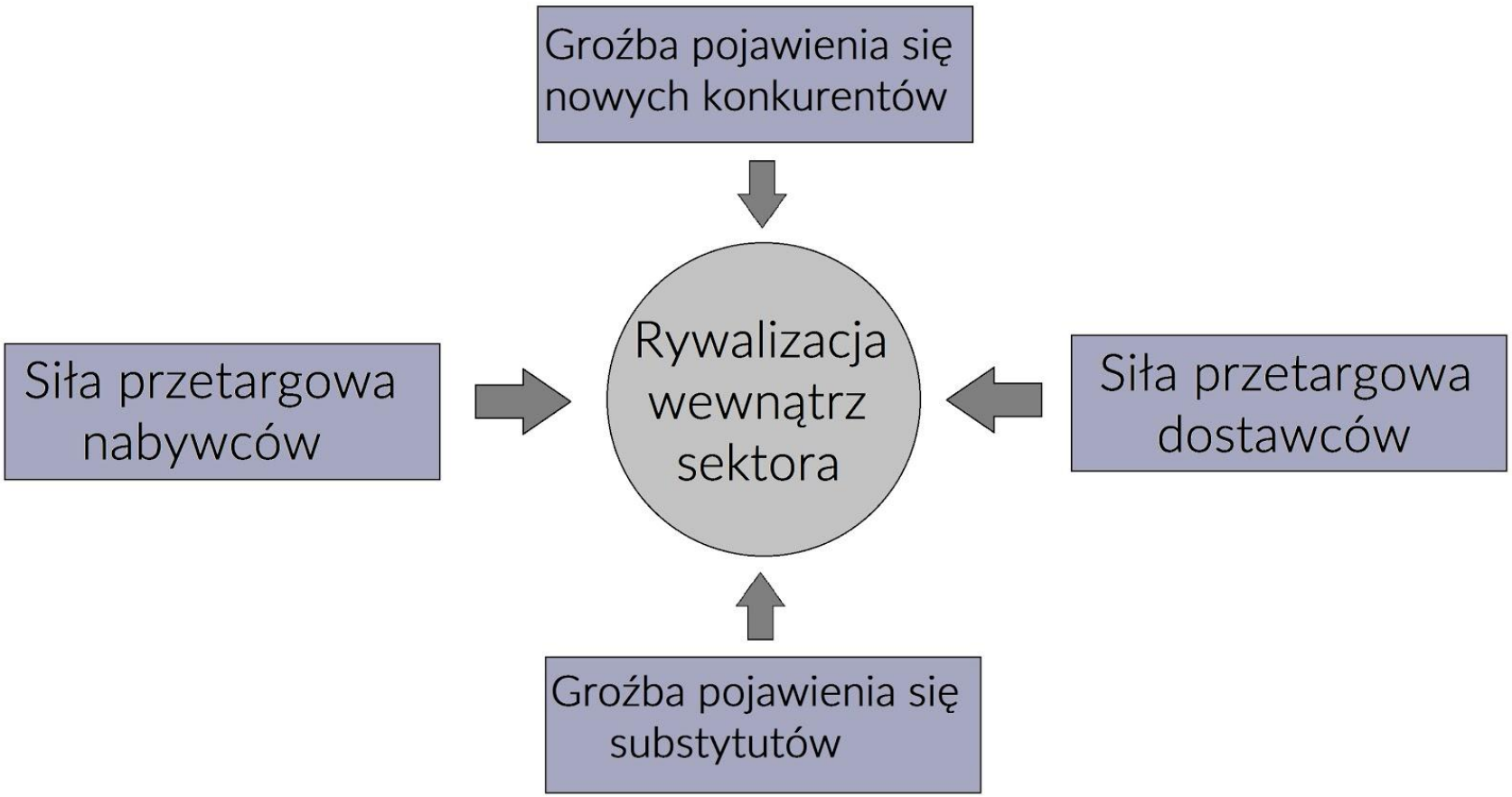
Analiza makrootoczenia

- Badanie sytuacji makro obejmuje aspekty:
  - prawne,
  - polityczne,
  - technologiczne,
  - społeczne.
- Badanie makro można przeprowadzić za pomocą analizy PEST.

5 Sił Portera

- Koncepcja 5 Sił Portera została opracowana przez Michaela E. Portera.
- Stosujemy ją rozważając wejście na dany rynek.
- Metoda służy do oceny atrakcyjności sektora i opiera się na 5 różnych czynnikach, związanych z otoczeniem, w którym funkcjonuje przedsiębiorstwo:
  1. siła przetargowa dostawców,
  2. siła przetargowa nabywców,
  3. natężenie walki konkurencyjnej wewnątrz sektora,
  4. groźba pojawienia się nowych producentów,
  5. groźba pojawienia się substytutów.

5 Sił Portera - relacje



Rysunek 3: Zależności między siłami Portera [3]

Opis Sił Portera

1. siła przetargowa dostawców,
   - Czy dostęp do materiałów jest prosty i czy są one tanie?
2. siła przetargowa nabywców,
   - Czy łatwo pozyskać klientów i sensowny udział w rynku?
3. natężenie walki konkurencyjnej wewnątrz sektora,
   - Jacy są główni gracze? Jak wygląda rywalizacja między nimi?
4. groźba pojawienia się nowych producentów,
   - Jakie są szanse na pojawienie się nowych graczy?
5. groźba pojawienia się substytutów.
   - Czy istnieją zamienniki dla naszych produktów?

Sposób mierzenia sił

- Siły nie muszą być bardzo precyzyjnie mierzone.
  - Skala Likerta (mała - duża).
  - punkty (1 - 10)
- W celu określenia poszczególnych wartości pomocne może być określenie aktualnej fazy sektora.
  - wschodzący,
  - rozwijający się,
  - dojrzały,
  - schyłkowy.
- Określenie groźby pojawienia się nowych konkurentów można dokonać poprzez analizę barier.

Początkowe fazy sektora

- Wschodzący
  - niepewność i ryzyko
  - niskie bariery wejścia do sektora
  - wysokie znaczenie technologii i innowacyjności
  - ograniczona konkurencja
  - ograniczony przepływ informacji
  - wysokie i zmienne ceny
  - działalność niedochodowa, ujemna płynność finansowa
  - duże potrzeby kapitałowe na finansowanie działalności
- Rozwijający się
  - szybko rosnący popyt
  - napływ nowych firm i wzrost konkurencji
  - szybki wzrost rentowności
  - gwałtowny spadek cen
  - działalność coraz bardziej zyskowna.

Końcowe fazy sektora

- Dojrzały
  - duże znaczenie reklamy
  - słabnący wzrost popytu nabywców
  - ostra walka konkurencyjna
  - obniżka cen
  - klienci bardziej wybredni
  - spadek dochodu
  - spadek rentowności
  - konieczność doskonalenia technologii
- Schyłkowy
  - stagnacja rynku
  - stabilizacja cen
  - sprzedaż na poziomie gwarantującym przetrwanie
  - opuszczanie sektora przez firmy
  - pozostanie kilku firm obsługujących rynek
  - omijanie konkurencji
  - niskie dochody, niewielka płynność finansowa

Bariery wejścia na rynek

- Korzyści skali,
- Kapitałochłonność,
- Know-how,
- Koszty zmiany dostawcy przez klienta,
- Zróżnicowanie produktów konkurencji,
- Bariery prawne.

Ograniczenia metody 5-ciu sił

- Analiza 5-ciu sił Portera jest często rozszerzana o analizę aliansów strategicznych, które zmieniają sytuację konkurencyjną.
- Model nadaje się do wykorzystania w przypadku analizy jednego rynku jednolitych, podobnych lub powiązanych produktów.
- Model został stworzony z myślą o statycznych stabilnych rynkach.
- Metoda jest jedynie początkowym schematem wykorzystywanym podczas analizy danego rynku.

PEST

- Koncepcję PEST opracował Francis Aguilar.
- Analiza PEST jest szczególnie pomocnym narzędziem dla przedsiębiorstw, które dopiero rozpoczynają działalność lub planują ekspansję na rynki zagraniczne.
- Nazwa jest akronimem czterech angielskich słów, które oznaczają poszczególne otoczenia przedsiębiorstwa
  1. otoczenie polityczne (Political)
  2. otoczenie ekonomiczne (Economic)
  3. otoczenie socjokulturowe (Social/Socio-cultural)
  4. otoczenie technologiczne (Technological)

Otoczenie polityczne

- Rozpatrujemy wszelkie kwestie związane z sytuacją polityczną oraz prawną kraju, w którym planowana jest działalność.
  - stabilność polityczna kraju,
  - system podatkowy,
  - cła i blokady,
  - proces rejestracji przedsiębiorstwa
  - przepisy związane z zatrudnianiem pracowników.

Otoczenie ekonomiczne

- Rozpatrujemy wszelkie kwestie związane z dotyczące sytuacji gospodarczej kraju, w którym planowana jest działalność.
  - poziom stóp procentowych,
  - inflacja,
  - wzrost gospodarczy,
  - stopa bezrobocia,
  - wartość segmentu, prognozy z nim związane i trendy na nim panujące.

Otoczenie socjokulturowe

- Rozpatrujemy wszelkie kwestie związane z demografią mentalnością ludności kraju, w którym planowana jest działalność.
  - faza rozwoju demograficznego społeczeństwa (stopa urodzeń i zgonów),
  - preferowany styl życia konsumentów,
  - tradycje i zwyczaje,
  - poziom edukacji,
  - zwyczaje zakupowe,
  - świadomość zdrowotna,
  - panująca struktura rodzinna,
  - podejście społeczeństwa do towarów zagranicznych i krajowych.

Otoczenie technologiczne

- Rozpatrujemy wszelkie kwestie związane z rozwojem technologicznym kraju, w którym planowana jest działalność.
  - poziom innowacyjności kraju,
  - wszelkiego rodzaju zachęty podatkowe związane z działalnością B+R,
  - istnienie nowych technologii, z których przedsiębiorstwo może korzystać,
  - dostęp konkurentów do nowych technologii, które mogą zmodyfikować ich produkty,
  - priorytetowe obszary będące celem polityki innowacyjności kraju.

Określenie szans i zagrożeń

- Po określeniu czynników występujących w makrootoczeniu przedsiębiorstwa należy ocenić, które z nich będą miały pozytywny (szanse), a które negatywny (zagrożenia) wpływ na działalność firmy.
- Ostatnim etapem analizy PEST jest określenie działań mających na celu wykorzystanie istniejących szans i uniknięcia zagrożeń.

Analiza konkurencji

- Analiza konkurencji jest użyteczna przy wejściu na istniejący rynek.
- Jej celem jest dostarczenie nam kompleksowej informacji na temat potencjalnych rywali.
- Obejmuje następujące obszary:
  1. Produkty i usługi
  2. Klienci
  3. Kanały sprzedaży
  4. Grupa docelowa
  5. Przewaga konkurencyjna
  6. Finansowanie
  7. Mocne i słabe strony

Produkty i usługi konkurencji

- Podstawą jest znajomość specyfikacji i cen usług oferowanych przez konkurencję.
- Ustalenie które produkty są najbardziej popularne?
- Ustalenie jaka cechy sprawiają, że oferta jest konkurencyjna?
  - cena,
  - jakość,
  - sposób dystrybucji,
  - unikalna wartość dodana.
- Znajdź elementy, które będą w Twoim produkcie i wyszczególnij te, które dają Ci przewagę.
- Możesz wykorzystać analizę morfologiczną.

Klienci

- Analiza charakteru i liczby klientów konkurencji.
- Analiza obecnych i historycznych danych, aby przeanalizować trendy.
- Ustalenie, poprzez analogię, ile czasu zajmie osiągnięcie określonej liczby klientów.

Kanały sprzedaży

- Ustalenie jakimi kanałami konkurencja sprzedaje produkty i usługi.
  - Czy są one zróżnicowane?
  - Czy sprzedaż jest prowadzona bezpośrednio?
  - Gdzie są ulokowane placówki dystrybucji?

Grupa docelowa

- Ustalenie liczebności i dominujących cech odbiorców produktów i usług.
- Pozwala na dostosowanie strategii marketingowych.
- Należy określić charakter socjo-demograficzny grupy.
  - styl życia,
  - rozmieszczenie geograficzne,
  - poziom lojalności do produktu.

Przewaga konkurencyjna

- Określenie przewagi konkurencyjnej lub niszy rynkowej.
  - Co pozwala wyróżnić się naszemu produktowi?
  - Czy produkt ma szansę zaistnieć na rynku?
  - Czy klienci dostrzegą co go wyróżnia?
- Spróbuj wykreować przewagę konkurencyjną
  - cena,
  - unikatowa cecha.

Finansowanie

- Określenie możliwości finansowania produktu.
- Realizowane poprzez analizę konkurencji, która odniosła sukces.
  - Kiedy konkurencja otrzymała dofinansowanie?
  - W jakich okolicznościach?
  - Od jakiego inwestora?

Mocne i słabe strony

- Podsumuj zdobyte informacje zestawiając mocne i słabe strony konkurencji.
- Można wykorzystać analizę SWOT.
  - plusy i minusy
  - szanse i zagrożenia.

Analiza morfologiczna

1. Zdefiniuj cechy produktów, które analizujesz.
2. Zdefiniuj wartości poszczególnych cech.
3. Określ ograniczony zestaw konfiguracji przeznaczony do analizy.

Geographic priority	Functional priorities	Size and cramming	New construction	Maintenance	General philosophy
Metropoles	All socio-tech. functions	Large, not crammed	With new construction	More frequent maintenance	All get same shelter quality
Cities + 50,000	Tech support systems	Large & crammed	Compensation	Current levels	All take same risk
Suburbs and countryside	Humanitarian aims	Small, not crammed	New only for defence build up	No maintenance	Priority: Key personnel
No geo-priority	Residential	Small & crammed			Priority: Needy

Rysunek 4: Analiza morfologiczna [5]

Model ewaluacji

- Nadanie cechom rank i skalując wartości możemy przeprowadzić ocenę rozwiązania.

TABLE 7.2 An Example of Vendor Analysis

Attributes	Rating Scale				
	Importance Weights	Poor (1)	Fair (2)	Good (3)	Excellent (4)
Price	.30				x
Supplier reputation	.20			x	
Product reliability	.30				x
Service reliability	.10		x		
Supplier flexibility	.10			x	
Total Score: .30(4) + .20(3) + .30(4) + .10(2) + .10(3) = 3.5					

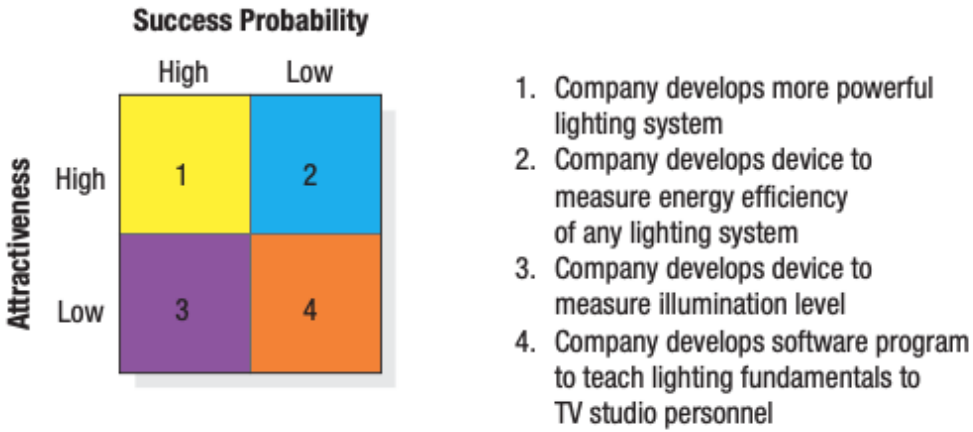
Rysunek 5: Ocena na podstawie morfologii [1]

Analiza SWOT

- Analiza SWOT to globalna ocena firmy, jej atutów i słabości, możliwości i zagrożeń.
- Jest narzędziem do monitorowania zewnętrznych i wewnętrznych czynników rynkowych.

Analiza możliwości rynkowych

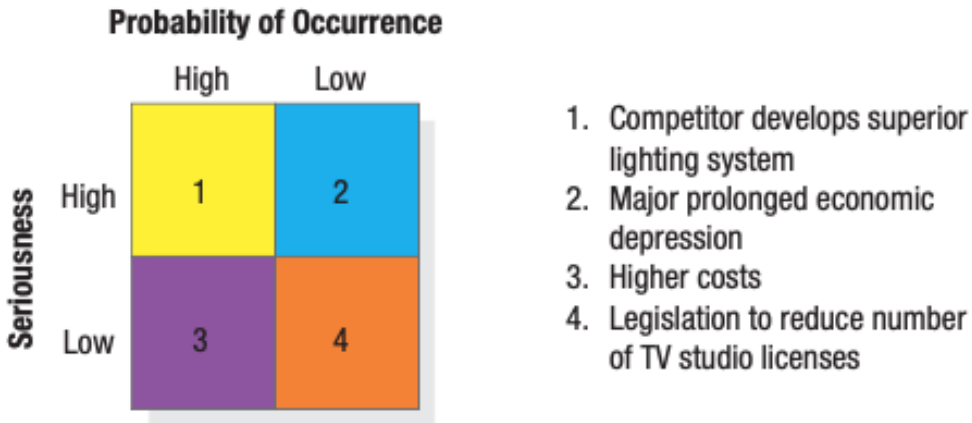
- Analiza możliwości rynkowych zestawia możliwości biznesowe pod kątem:
  - Możliwości osiągnięcia sukcesu.
  - Atrakcyjności.



Rysunek 6: Macierz możliwości [1]

Analiza zagrożeń

- Analiza zagrożeń analizuje rynek pod kątem:
  - Możliwości wystąpienia zagrożenia.
  - Powagi zagrożenia.



Rysunek 7: Macierz zagrożeń [1]

Bibliografia I

P. Kotler and K. K. Lane.

Marketing Management.

Pearson Education, 2016.

W. Lika.

Osint, czyli biały wywiad – metoda pozyskiwania informacji z cyberprzestrzeni w oparciu o dane jawnoźródłowe.

J. Osiadacz.

Narzędzia identyfikacji potrzeb innowacyjnych w przedsiębiorstwach.

PARP, 2011.

R. A. P. Rico, M. J. H. Medina, C. C. P. Hernández, D. O. D. López, and J. C. C. G. Ruíz.

Use of osint in a colombian context and sentiment analysis.

Revista Vínculos: Ciencia, Tecnología y Sociedad, 15(2), 2018.

Bibliografia II

T. Ritchey.

General morphological analysis* a general method for non-quantified modelling.

Swedish Morphological Society, 2002.

K. Tylutki.

Informacja masowego rażenia – osint w działalności wywiadowczej.

Przegląd Bezpieczeństwa Wewnętrznego, 19, 2018.